PRICEWATERHOUSECOOPERS

HIPAA's Myths, Practical Realities and Opportunities:

The Work Providers Need to Perform For Standard Transactions and Code Sets

Jeff Fusile
Tom Hanks
Jon Neiditz

January 2002

- Jeffrey P. Fusile, National Partner in Charge of PwC's HIPAA Consulting Services

  (678) 419-1558, Jeff.Fusile@us.pwcglobal.com
  Jeff serves as National Partner in Charge of PwC's HIPAA Consulting Services. He is responsible for the firm's nationally integrated practice of more than 200 professionals dedicated to the HIPAA issue. Since 1999, Jeff has focused almost 100% of his time to helping organizations address the challenges and opportunities associated with HIPAA's Administrative Simplification provisions. Jeff has provided significant HIPAA assistance to many of the nations largest healthcare organizations.

  Jeff is a frequent author and speaker on the subject of HIPAA, he has been asked on numerous occasions to provide practical insight to many inside the beltway, including both U.S. Senators and Representatives, and he has testified on several HIPAA related issues in front of the National Council for Vital Health Statistics (NCVHS). Jeff is also recognized for his knowledge on the subject of healthcare privacy and serves on the advisory council for the Privacy Officer's Association. Prior to HIPAA, Jeff concentrated his efforts in several key areas, including strategic planning, business process improvement, regulatory compliance, information technology, and litigation support services all focused within the healthcare industry.

- Thomas L. Hanks, Director, HIPAA Consulting Services

  (312) 298-4228, thomas.l.hanks@us.pwcglobal.com
  Tom has over twenty years of management consulting, information systems, and operations experience. Tom is a nationally recognized authority on the Administrative Simplification section of the Health Insurance Portability and Accountability Act (HIPAA). This section of HIPAA establishes rules and standards for electronic transactions, healthcare identifiers, security, and privacy of health information. Since 1995, Mr. Hanks has been actively contributing expertise to industry associations and working with the Department of Health and Human Services (DHHS) personnel addressing compliance with HIPAA regulations.

- Jonathan Neiditz, Director, HIPAA Consulting Services

  (678) 419-1556, jonathan.a.neiditz@us.pwcglobal.com
  Jon has over 16 years of experience leading strategic initiatives in health and healthcare. Jon's practice at PwC focuses on HIPAA implementation and privacy more generally. He is also an experienced transactional and regulatory attorney. He has led or is leading HIPAA privacy engagements for such clients as Aetna, Ford and ValueOptions/FHC.

TABLE OF CONTENTS

Executive Summary

Many segments of the health care industry—particularly physicians, hospitals and other health care professionals (for brevity, physicians, hospitals and other health care providers are referred to broadly as "providers" throughout this article)—have not fully come to grips with the challenges imposed by HIPAA's standard transactions and code set (TCS) requirements. This is not to say that all providers are behind, some are clearly not. However, the vast majority of providers are considerably behind where they should be at this point in the HIPAA TCS process.

The purpose of this document is to dispel some of the popular myths circulating about HIPAA and shed light on the scope and magnitude of the effort providers will need to undertake to achieve even basic compliance with HIPAA's TCS requirements. Further, we try to clarify the distinction between basic compliance and real administrative simplification. Some argue that the ideal solutions for administrative simplification in the short-term may already be lost for many providers due to the lack of focus and the impending time pressure to achieve even basic compliance by October 16, 2002.

It is the view of PricewaterhouseCoopers, as one consulting firm helping its clients address HIPAA, that implementing HIPAA's standard transactions and code sets requires focused and consistent effort over a significant period of time—with the period of time varying dramatically based on each organization's particular circumstances and objectives. Many obstacles arise, some anticipated and some unanticipated, as one drills down into the details. It is in these details where the real challenges and opportunities reside.

The following is a summary of the issues addressed in the main body of this document:

MYTH #1: **"The only thing physicians, hospitals and other health care providers ("providers") need to do is to contract with a clearinghouse to achieve HIPAA compliance."**

REALITY: Regardless of whether a provider uses a clearinghouse, the provider will have to do much of the work needed to achieve compliance itself, including collecting and submitting much more data than today, training its staff on the new medical and non-medical codes, assessing and modifying many of its operations to address the "ripple" effect, and integrating the data into its operations. Providers still need to perform the lion's share of the work regardless of whether they use a clearinghouse.

Clearinghouses can deliver valuable services to providers in many contexts. For example, clearinghouses enable providers needing to communicate with many small commercial payers the ability to conduct these transactions through a single submission point. However, it may not be in the providers' best interest to be put in a position in which their only choice is to use a clearinghouse for submission and routing of all transactions. It often will not make sense for providers to stop short of being capable of producing and transmitting their own transactions directly to payers, especially to those payers with whom they have significant volume. Further, this flexibility will provide them significant options and negotiating leverage with both the payers and the clearinghouses.

MYTH #2: **"Vendors can deliver HIPAA compliance to providers via software."**

REALITY: While some vendor products will certainly facilitate compliance, no vendor can make a covered entity compliant through software. Providers themselves must perform a substantial amount of the work necessary to achieve compliance with TCS, including:

- **collecting and submitting incrementally more and different data elements for claims and other transactions, than are commonly collected and submitted today;**

- **assessing and remediating the providers' many systems that will be impacted by the "ripple effect" – changes needed to providers' core systems will necessitate corresponding changes throughout the providers' systems and operating environment;**

- **assessing the impact of the elimination of local medical and service codes on a provider's revenues; and**

- **training staff on the new data requirements, including both the medical/service codes and the new non-medical codes (e.g., marital status, relationship codes, adjustment reason codes, etc.).**

Many vendors who are making significant investments are not adequately communicating their intentions and may be reluctant to communicate details because of potential legal liability. This means that it is difficult for providers to differentiate those vendors that are making adequate investments in TCS from those vendors who may not be making adequate investments. On the other hand, what may be more troublesome are vendors claiming "HIPAA compliance" without communicating specifics.

In fact, any vendor who claims to be HIPAA compliant - or worse yet, that use of their product(s) will make a client/customer HIPAA compliant – does not understand HIPAA. It is in a vendor's self interest to provide comfort to providers at this stage when, in reality, many vendors are wrestling with compliance themselves, including not only how they will facilitate, but also when they will be ready. Few providers know specifics about what their vendors are doing and planning to offer, yet many are relying on the vendor for substantial compliance with transaction standards and code sets.

MYTH #3: **"Many providers are already HIPAA compliant with these transactions; what's the big deal?"**

REALITY: The technical nature of this issue has led some providers to believe that they are already performing HIPAA standard transactions. However, they are almost always using only one or two of the many HIPAA standard transactions and are nearly always using earlier versions of these transactions, not the HIPAA-mandated versions.

These providers are often unaware of the significant differences between general ASC X12N transactions and the more detailed requirements of HIPAA standards for each transaction, as articulated in the specific HIPAA implementation guides. Further, many providers incorrectly believe that their clearinghouse or system vendor already has this capability and is already converting to HIPAA standard transactions. This is generally not true. Further yet, most providers have overlooked the critical need for testing. Providers need to conduct testing with each payer for a variety of transactions, not only for the format and content that is specifically required, but also for any optional data elements that may be agreed to contractually. In addition, many provider systems currently contain logic to create payer-specific coding to accommodate payer- or plan-specific code sets. With the elimination of non-standard codes, providers must "unwind" payer-specific coding issues and implement new process to track and submit non-standard yet required data. We are particularly concerned that few providers have assessed the effect this code set conversion will have on their specific reimbursement levels.

MYTH #4: **"The industry will have had more than the required 24 months to implement administrative simplification."**

REALITY: This argument is misleading and mischaracterizes the HIPAA standards. There have been many significant proposed and approved changes to the HIPAA transaction standards and code set regulations. In fact, we are currently anticipating updates to certain standards as this document goes to print. What is more important to note is that final rules, in this instance, will not mean that there will be no additional changes to this component of HIPAA. While we understand why many have hesitated to start, we suggest that this normally prudent "wait and see" behavior is no longer acceptable in addressing HIPAA TCS regulations given the time remaining.

MYTH #5: **"Medicare already does it, therefore it should translate easily into other government and private pay situations."**

REALITY: While Medicare does use an earlier version of the claim transaction (837) and remittance transaction (835), it does not use all of the mandated HIPAA standards. Further, there are significant differences in the earlier versions of the claim (837) and remittance (835) transactions from the mandated HIPAA standard formats. As a result, Medicare also must make significant investments to achieve HIPAA compliance. Compared to private payers, Medicare's changes, while extensive, are less complex than those faced by private payers and Medicaid. However, providers will face substantial changes to their operations, including collecting and submitting many new and different data elements (including those not currently needed for Medicare) and using all the standard medical and non-medical codes in order to submit HIPAA compliant claims and other transactions to Medicare.

The Medicare program's use of ANSI X12N standards for some transactions does not constitute a basis of comfort for providers engaged in certain electronic transactions with Medicare and seeking to move to HIPAA compliant transactions. To be compliant, HIPAA standard transactions (except for retail pharmacy, which utilizes an entirely different standard known as NCPDP) must not only conform to the ANSI X12N version 4, release 1, sub-release 0 ("004010," as opposed to the much more widely used version "003051," the version currently utilized by Medicare), but must also conform to the appropriate HIPAA transaction implementation guide. Many differences between Medicare's implementation of the ANSI transactions and the requirements of HIPAA's implementation guides exist, and the differences even among the Medicare's implementation of the ANSI standards are significant. The largest difference between Medicare and non-Medicare transactions for HIPAA implementation purposes is the degree of centralization and uniformity of Medicare systems. Non-Medicare systems, by contrast, often have to deal with many conflicting legacy systems, as well as local and client-specific requirements not faced by the Medicare program, including many "workarounds" designed to address the needs of a particular customer, particular provider or particular market.

MYTH #6: "HIPAA Compliance will be much simpler for small providers."

REALITY: The evidence does not support this statement. In fact, some have suggested that their issues may be more challenging. Small providers are often, even today, unaware of HIPAA and the magnitude of its effects.

The only basis for this argument that compliance will be much simpler for small providers seems most often linked to the ability of small providers to revert to paper/manual transactions. This course of action may prove comforting in the short-term, but over the long-term may prove to be crippling. In fact, CMS has indicated that they may begin charging a fee for the processing of paper claims submissions, which would likely open the door to fees being charged by all healthcare payers.

MYTH #7: "State governments only need to worry about Medicaid and their state employee group health plans."

REALITY: State governments are coming to realize the broader impact of HIPAA. In fact, the National Governors Association (NGA) recently noted that "all state agencies that collect health data, provide or pay for health services, conduct research, or develop health policy will need to comply with HIPAA uniform standards in order to conduct business and protect public health." Few states or federal agencies have assessed the impact of HIPAA in this manner, or budgeted for an assessment or for the changes that will soon be required. Many government agencies, instead of carefully analyzing the information they can get through the new standard transactions, will simply impose new reporting requirements outside of the HIPAA standard transactions. As a result, in addition to the efforts required for HIPAA compliance, providers will need to be educated and will need to develop new procedures to comply with these new government reporting processes and requirements.

MYTH #8: "HIPAA compliance equals administrative simplification."

REALITY: This statement is simply not true; compliance can be obtained without realizing any operational efficiency or simplification. For that matter, compliance could be obtained while becoming less efficient and more complex. HIPAA offers no guarantees for improved efficiency or administrative simplification; these things will only come to those who seek them carefully and diligently. Make no mistake: HIPAA is a watershed event for the healthcare industry, but there are no assurances that its benefits will be evenly distributed; instead, they will cluster around those organizations that are most effectively prepared for them.

Introduction[1]

The purpose of this document is to dispel some of the popular myths circulating about the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and shed light on the scope and magnitude of the effort providers will need to undertake to achieve even basic compliance with HIPAA's standard transaction and code set (TCS) requirements. Further, we try to clarify the distinction between basic compliance and real administrative simplification. This article is focused exclusively on the HIPAA TCS regulations; it does not attempt to address HIPAA's final privacy regulations, its proposed security regulation, or its' pending regulations regarding unique identifiers or enforcement. This document focuses primarily on the readiness of providers because they are critical to the success of administrative simplification.

First, a quick comment about our perspective. We are consultants with PricewaterhouseCoopers, the largest professional services firm in the world, and the leading HIPAA consulting practice in the nation. The PricewaterhouseCoopers HIPAA Consulting Practice is a nationally integrated practice, comprising over 200 professionals and includes many recognized experts in standard transactions and code sets, privacy, security, project management and education. The group is fortunate to include some of the industries most recognized thought leaders on HIPAA's administrative simplification provisions. In addition, the group continues to build on its strengths, as evidenced by the addition of HIPAA's most accomplished professional, Dr. Bill Braithwaite. Dr. Braithwaite selected PricewaterhouseCoopers, from a variety of organizations, as the organization he believes to be in a strong position to help bring about real and positive change for its clients as well as for the broader healthcare industry.

Our HIPAA practice assists insurance organizations, provider entities, employers, government agencies, pharmaceutical companies, research organizations, public-private partnerships and community health organizations address the challenges and opportunities of HIPAA in ways that best enable those organizations to fulfill their missions and meet their goals. We have experienced firsthand the important lessons that can only be learned in the "trenches" of HIPAA implementation. We are excited to be on the forefront of understanding how HIPAA can be most effectively integrated into the operations of our clients, and how HIPAA will ultimately impact the entire healthcare landscape.

Our extensive experience has taught us that HIPAA's "good things" do not come to those who wait, but require careful planning and hard work. Moreover, HIPAA must be carefully woven into the fabric of organizations, through recognizing the difference between HIPAA requirements, interoperability requirements—the ways in which the pieces fit together in an organization—and business needs, and paying adequate attention to all three. In other words, just because HIPAA has standard implementation guides, do not think there is such a thing as a standard implementation.

1 We thank Dr. Kepa Zubeldia, Bob Stallings, James Barnard, Steven Barr, Jack Joseph, and Maria Ward for their contributions to this article.

The intent of HIPAA's Administrative Simplification provisions was to promote the affordability of health care services and insurance coverage through improving administrative operations in the health care system. On August 17, 2000, the Department of Health and Human Services issued final rules for the standardization of the form and content of the following electronic healthcare transactions:

- Claims and encounter transactions;
- Coordination of benefits;
- Enrollment and disenrollment;
- Eligibility inquiries;
- Payment and remittance advice;
- Premium payments;
- Claims status inquiries;
- Referral authorizations; and
- Retail pharmacy.

The rules also addressed the code sets providers and health plans will be required to use for data included in the above identified transactions as well as in future transactions that HIPAA may bring forth. Code sets refer to two primary categories of codes, the more obvious clinical codes (i.e., ICD-9, CPT-4, HCPCS, etc), but also the less understood supporting codes (often referred to as valid values) utilized within the transaction (i.e., marital status codes, retiree codes, gender). These new rules clearly eliminate the use of local codes when submitting data electronically. Local codes are those codes created to address specific payer and provider issues. They have been created over time to address the unique needs of a particular customer, particular payer or provider or particular market. They are also used to identify and pay for new technologies and procedures when a national code has not yet been made available.

Effective October 16, 2002, all regulated entities are expected to come into compliance with these standards. The rules take advantage of standards set by private volunteer standard-setting bodies, coordinated through the X12 Accredited Standards Committee of the American National Standards Institute (ANSI), but exceed those standards in their specificity.

This article attempts to present a clear view of the substantial work that lies ahead for the healthcare provider community. This view is based on our experience with helping a variety of clients with HIPAA, our broad knowledge of healthcare operations, and our leadership in the healthcare industry from both a commercial and a governmental perspective. We hope our analysis will help readers understand HIPAA implementation as both very challenging and very worthwhile.

Our view is that implementing HIPAA's standard transactions and code sets requires focused and consistent effort over a significant period of time—with the period of time varying dramatically based on each organization's particular circumstances. Many obstacles arise, some anticipated and some unanticipated, as one drills down into the details. The sooner this concerted effort takes place, the more likely organizations are to achieve an acceptable level of compliance, and the more likely they will have the time to integrate real administrative savings into their operations and ultimately improve their competitive position. However, given the compliance date is now less than one year away, any organization that has not started its HIPAA compliance efforts is in serious jeopardy of failing to achieve an acceptable level of HIPAA compliance, much less realize any administrative simplification. Failure to achieve an acceptable level of HIPAA compliance could have a significant impact on an organization's operations and corresponding cash flow.

We will respond to many of the statements that are made indicating that HIPAA compliance is easy. Many of these statements, like this article, are well-intentioned efforts to move HIPAA compliance forward. However, while the intention of these statements is rarely if ever to dissuade providers and others from getting to work on HIPAA, we have seen them have just such an effect. We believe it is important to develop a shared understanding of the work that needs to be done, and hope this article contributes to such an understanding.

A few things that this article is not: First of all, a reminder - this article does not address HIPAA's privacy and security rules—they will be addressed elsewhere. Secondly, it is not a research paper, but a reflection of real experiences in the marketplace. That method has advantages and disadvantages. We have used it here in part because much of the published research in the area of HIPAA readiness (including our own) relies on readiness surveys. We believe that the responses to such surveys are often limited in value by the absence of a shared understanding of the work that needs to be done, and in fact may often be biased by the very HIPAA myths addressed in this article.

Provider Myths and Realities

MYTH #1: "The only thing providers need to do is to contract with a clearinghouse to achieve HIPAA compliance."

REALITY:

Summary:

Regardless of whether a provider uses a clearinghouse, the provider will have to do much of the work needed to achieve compliance itself, including collecting and submitting much more data than today, training its staff on the new medical and non-medical codes, assessing and modifying many of its operations to address the "ripple" effect, and integrating the data into its operations. Providers still need to perform the lion's share of the work regardless of whether they use a clearinghouse.

Clearinghouses can deliver valuable services to providers in many contexts. For example, clearinghouses enable providers needing to communicate with many small commercial payers the ability to conduct these transactions through a single submission point. However, it may not be in the providers' best interest to be put in a position in which their only choice is to use a clearinghouse for submission and routing of all transactions. It often will not make sense for providers to stop short of being capable of producing and transmitting their own transactions directly to payers, especially to those payers with whom they have significant volume. Further, this flexibility will provide them significant options and negotiating leverage with both the payers and the clearinghouses.

Supporting Information:

This pronouncement is not only misleading, it may prove dangerous if it dissuades providers from doing the necessary analyses to identify needed operational and contractual changes. While clearinghouses will serve as an acceptable and valuable mechanism to convert non-standard data into HIPAA compliant data and vice versa, there is a significant amount of work to be done to enable the clearinghouse to successfully perform these tasks. Many providers often fail to recognize that a clearinghouse needs to be provided nearly all of the relevant data in order to perform this conversion. Many providers have not yet come to understand what data needs to be provided and under what circumstances. As an example, let's look at the HIPAA standard claims transaction. With the exception of Pharmacy claims (which utilize a unique NCPDP format), there are three standard claim types (institutional, professional and dental) under HIPAA known generically as the 837 transactions. We will focus on the 837I (the institutional claim) as a proxy for all three types of claims.

The 837I claims transaction is defined by the HIPAA Implementation Guide entitled "Health Care Claim: Institutional;" it is a 634-page technical document. There is a specific Implementation Guide for each of the HIPAA standard transactions, including separate guides for the professional and dental claims transactions. We will not attempt to address the technical issues included within each of these guides, but rather focus on selected issues within the guide that all providers need to understand.

Many providers often ask simply for the minimum data set for a standard HIPAA compliant transaction; a specific number and type of field elements that can always be provided to ensure that they meet HIPAA's minimum requirements for an acceptable claim. No such minimum data set exists. There are over 900 fields that in a variety of situations may be required to generate a HIPAA compliant facility transaction. However, never will all of these fields be required together. What then is the minimum data required for a compliant HIPAA facility claim? As was previously noted, there is no minimum data set, but there are 126 fields that are required to be in each and every possible configuration of a HIPAA compliant facility claim. However, it is important to note, all 126 of these fields taken together will never be enough, on their own, to generate a HIPAA compliant claim. For a listing of these "always required" fields see Appendix I.

It is also important to note that many of these fields are incremental to those utilized today. Further, many of the fields that are utilized today are now being formally redefined by HIPAA's data element dictionary. This data element dictionary will serve to standardize what is meant by each field, just as the corresponding implementation guide for each transaction defines the acceptable values and format that can be utilized to populate each of these fields. To further explain this point we will try to clarify with a specific example. Let's assume that a patient presents to the hospital for admission. The admissions clerk will need to know the relationship the patient has to the subscriber of record on the insurance that is presented. This field, "individual relationship code" is a required field and HIPAA defines the acceptable inputs for a compliant HIPAA claim. The acceptable inputs for the "individual relationship code" are as follows:

- 01 Spouse
- 04 Grandfather or Grandmother
- 05 Grandson or Granddaughter
- 07 Nephew or Niece
- 10 Foster Child
- 15 Ward
- 17 Stepson or Stepdaughter
- 18 Self
- 19 Child
- 20 Employee
- 21 Unknown
- 22 Handicapped Dependent
- 23 Sponsored Dependent
- 24 Dependent of a Minor Dependent
- 29 Significant Other
- 32 Mother
- 33 Father
- 36 Emancipated Minor
- 39 Organ Donor
- 40 Cadaver Donor
- 41 Injured Plaintiff
- 43 Child Where Insured Has No Financial Responsibility
- 53 Life Partner
- G8 Other Relationship

This scenario, while not new, will require certain changes on the part of the admissions clerk. Ideally, it will lead to new processes, data entry screens, manual forms and/or enhancements to current training curriculums. For instance what new procedures and training will be required for the admission clerk to distinguish between emancipated minors and a foster child or between spouse, significant other and life partner. This is one simple example to show the operational challenges that HIPAA will present. There are literally hundreds of similar scenarios. This is not simply a technology issue, it will impact almost all areas of operations and providers need to begin preparing for these changes.

The omission of one required field or the inclusion of any non-valid data into a particular field renders the transaction non-compliant. Further, while many have assumed that certain payers will continue to accept specific transactions in the old (pre-HIPAA) format, the federal government seems to think otherwise. In a submission to the frequently asked questions of the Department of Health and Human Services (HHS), dated September 17, 2001, the following question was asked:

"Is it permissible for health plans to continue to accept additional formats as well as the standard transactions adopted under HIPAA past the effective date of the final regulation?"

The answer was as follows:

"Section 162.923(a) of the regulation requires a covered entity that electronically conducts a transaction adopted under part 162 of the regulation, with another covered entity, to conduct the transaction as a standard transaction. Health plans may continue to accept additional electronic formats after the transaction and code set rule compliance date only if the submitter is NOT a covered entity under HIPAA."[2]

If providers cannot submit standard transactions that are entirely compliant in all respects, payers thus cannot accept them.

Whether or not they use a clearinghouse, providers need to consider the following issues:

(1) They need to understand and make operational changes necessary to identify, collect and populate the required data elements that they are not currently capturing, or are capturing but not transmitting. Some current electronic formats provide for many of these elements, but HIPAA often requires more data than is currently captured and stored. Providers should use this opportunity to reassess their business operations and clearinghouse relationships.

(2) Providers need to be aware of regulatory or accreditation requirements for data submission that is currently transmitted via non-standard transactions, but for which there is no place within the new HIPAA standard claims transaction. Will this situation require another transaction or will the requirement be modified? In the near term, multiple reporting requirements will apply. Such overlapping requirements are likely to proliferate with expanding epidemiological needs and other public health reporting requirements.

2 Available at http:/aspe.os.dhhs.gov/admnsimp/qdate01.htm

Examples of these types of requirements may include activities of daily living (ADLs) in nursing home claims, certain disease registries, DSM-IV codes for behavioral health claims, service rank for DOD and VA situations, and countless other state specific reporting requirements. To clarify, there are certain data elements that are considered important pieces of information that today are included in specific claims or other transactions. Going forward with standard HIPAA transactions, these data elements will no longer be permissible to include in the HIPAA standard transaction. These situations will create the need for new communication protocols, some will be communicated through new mechanisms and some will require paper submission in addition to the electronic transaction. Providers need to understand these new procedures and integrate them into their day-to-day operations.

Dealing with these operational and contractual changes is critical to realizing the potential benefits—or suffering the potential detriments—of HIPAA standard transactions, and can be even more labor-intensive than preparing for the submission and receipt of standard HIPAA formats.

If the great majority of the provider community indeed becomes reliant on clearinghouses for compliance in the early period of HIPAA implementation, many questions arise. For example:

What will that mean for clearinghouse pricing and the ability of providers to capture HIPAA-related savings? We believe that in the long run, HIPAA will drive down clearinghouse prices and make clearinghouses compete for books of provider business, but with a little more than a year to go until the standard transactions become effective, there appears to be little evidence of such price competition in the Clearinghouse market.

Under what circumstances will a contract with the clearinghouse hold the clearinghouse liable when the clearinghouse is unable to take responsive data from the provider and generate a HIPAA compliant transaction to the payer, or vice versa? In the clearinghouse industry, it is not uncommon for contracts to limit a clearinghouse's liability to the amount of fees.

To what extent will use of a clearinghouse relieve the provider of the burden of testing transactions, and to what extent is it necessary or prudent for the provider to test all transactions with the clearinghouse or even with each specific payer?

If the "all we need to do is contract with a clearinghouse" argument lulls providers into avoiding required duties, its impact on provider opportunities to improve their business processes and financial performance may be even more problematic. Only actively- engaged providers can take full advantage of such opportunities.

MYTH #2: "Vendors can deliver HIPAA compliance to providers via software."

REALITY:

Summary:

While some vendor products will certainly facilitate compliance, no vendor can make a covered entity compliant through software. Providers themselves must perform a substantial amount of the work necessary to achieve compliance with TCS, including:

- **collecting and submitting incrementally more and different data elements for claims and other transactions, than are commonly collected and submitted today;**
- **assessing and remediating the providers' many systems that will be impacted by the "ripple effect" – changes needed to providers' core systems will necessitate corresponding changes throughout the providers' systems and operating environment;**
- **assessing the impact of the elimination of local medical and service codes on a provider's revenues; and**
- **training staff on the new data requirements, including both the medical/service codes and the new non-medical codes (e.g., marital status, relationship codes, adjustment reason codes, etc.).**

Many vendors who are making significant investments are not adequately communicating their intentions and may be reluctant to communicate details because of potential legal liability. This means that it is difficult for providers to differentiate those vendors that are making adequate investments in TCS from those vendors who may not be making adequate investments. On the other hand, what may be more troublesome are vendors claiming "HIPAA compliance" without communicating specifics. In fact, any vendor who claims to be HIPAA compliant - or worse yet, that use of their product(s) will make a client/customer HIPAA compliant – does not understand HIPAA. It is in a vendor's self interest to provide comfort to providers at this stage when, in reality, many vendors are wrestling with compliance themselves, including not only how they will facilitate, but also when they will be ready. Few providers know specifics about what their vendors are doing and planning to offer, yet many are relying on the vendor for substantial compliance with transaction standards and code sets.

Supporting Information

The vendor community is uneven in its level of commitment and investment towards HIPAA compliance. Some vendors have invested heavily and are embedding into their systems HIPAA compliant data, transaction formatting and the corresponding data collection tools and reporting functionality. Other vendors have made little progress and are wrestling with even the most basic of HIPAA issues. We are concerned when we learn that providers are relying completely on their systems vendors, when we know that many vendors have done little to justify this reliance. We do not intend to portray a negative image of the vendor community, but rather to encourage the provider community to understand and challenge their vendors in relation to HIPAA compliance. Providers should have clearly articulated requirements, outlining specifically what they are expecting from their vendors. These requirements should be supported by a clear and well documented understanding of what each vendor is and is not going to do to meet these requirements. Providers will then know what they need to do to blend their operations with the considerable enhancements that will likely be required of their information systems.

Further compounding the vendor reliance issue is one of timing. On October 16, 2002 many providers will be required to use HIPAA's standard transactions. There is no grace period for providers who are not ready or who experience unanticipated complications. Many vendors have communicated that they will be issuing their "HIPAA friendly" versions sometime in the 1st or 2nd quarter of 2002. It is not at all clear that all systems vendors are developing HIPAA solutions that will produce and accept standard formats even by the standard transaction compliance date of October 16, 2002. Most institutional providers use one or more of the major health information systems (HIS). It is still uncertain whether and when these major HIS vendors will have HIPAA-enabled and properly tested versions of their software ready for migration. Whether these systems, once ready, will address only the data content of HIPAA transactions—or whether they will produce and receive the standardized HIPAA formats—is also unclear, and varies by vendor. This uncertainty hinders the ability of providers to properly plan for and implement HIPAA-compliant processes. Moreover, even if these systems are ready in time and produce and receive the standard transactions, the providers will still need time for upgrading and testing all permutations of the transaction types, and integrating their business processes with the new software. According to a recent article by Wes Rishel of the Gartner Group[3],

> *"HCOs must assess the impact of the HIPAA standard on all systems that provide data to – or use data from – the systems that create or process HIPAA transactions. Most of these systems will require at least some level of remediation. As enterprises assess the requirements for compliance with the HIPAA transaction, code and identifier standards, they must evaluate the impact on three categories of application systems:*
>
> *Transactors – systems that are the source or recipient of the HIPAA transaction*
>
> *Data feeders – systems that gather data and pass it to the transactors*
>
> *Data users – systems that make downstream use of information gathered by the transactors*

Data feeder systems may have to be changed to collect data that was not previously required, such as the birth date and gender of the subscriber. Data user systems may have to adjust to different codes as the transactors are remediated for HIPAA. In provider and payer enterprises, many application systems fit one or more of these categories. For example, patient registration

3 "Integration Architectures for HIPAA Compliance: From 'Getting it Done' to 'Doing it Right'," by Wes Rishel, Research Director Healthcare Industry Research & Advisory Service. The Gartner Group.

systems are transactors for eligibility, pre-certification and referrals; at the same time, they are data feeders for the billing system.

In a large enterprise, for each kind of application, there may be several (perhaps as many as a dozen) distinct instances of an application system. These distinct instances are usually different products, each of which must be assessed and remediated separately. In total, large integrated delivery networks may have to assess 100 or more distinct systems, and payer enterprises that have grown through acquisition may have to assess dozens."

Consequently, If a major systems vendor is not ready in time, a very large number of providers must find and contract with another vendor and undertake the complex and very time-consuming process of replacing one vendor with another; in most circumstances, this process is not a viable alternative given the short time frame under which this conversion would be required.

Further, it is even less clear how these vendors will leverage these new standard data formats to provide truly enhanced functionality to the provider community. The goal is not to simply implement a new form of electronic submission, but to leverage this new standard to drive real savings into the system. For example, will the vendor allow for on-line eligibility inquiry, or real-time claim status checks? The leveraging of these standards could save enormously on personnel time, and have the potential to improve an organization's cash flow, but it requires a step beyond compliance, and there is little evidence to show that vendors are focused in the near term on driving beyond simple compliance to the value HIPAA can provide.

MYTH #3: "Many providers are already HIPAA compliant with these transactions, what's the big deal."

REALITY:

Summary

The technical nature of this issue has led some providers to believe that they are already performing HIPAA standard transactions. However, they are almost always using only one or two of the many HIPAA standard transactions and are nearly always using earlier versions of these transactions, not the HIPAA-mandated versions.

These providers are often unaware of the significant differences between general ASC X12N transactions and the more detailed requirements of HIPAA standards for each transaction, as articulated in the specific HIPAA implementation guides. Further, many providers incorrectly believe that their clearinghouse or system vendor already has this capability and is already converting to HIPAA standard transactions. This is generally not true. Further yet, most providers have overlooked the critical need for testing. Providers need to conduct testing with each payer for a variety of transactions, not only for the format and content that is specifically required, but also for any optional data elements that may be agreed to contractually. In addition, many provider systems currently contain logic to create payer-specific coding to accommodate payer- or plan-specific code sets. With the elimination of non-standard codes, providers must "unwind" payer-specific coding issues and implement new process to track and submit non-standard yet required data. We are particularly concerned that few providers have assessed the effect this code set conversion will have on their specific reimbursement levels.

Supporting Information

Very few providers are submitting HIPAA compliant transactions today. Some providers believe themselves to be compliant or very near compliant with the standard transactions because they can submit a version of the 837 claims submission and receive a version of the 835 (remittance advice). These current 837 submissions are based on individual payers' implementation guides that have markedly different requirements than the now-definitive HIPAA implementation guides. To be compliant, HIPAA standard transactions (except for retail pharmacy which utilizes an entirely different standard known as NCPDP) must conform to the ANSI X12N - Version 4, Release 1, Sub-Release 0 ("004010"), as articulated in the HIPAA implementation guide. This "004010" version is considerably different than the "003051" version which is used by certain providers today and most notably by Medicare. The provider needs to look at the HIPAA implementation guide for the implications with regard to each element contained in each type of transaction. Without getting overly technical, the two basic differences between the "003051" and the HIPAA version of the "004010" transaction are as follows:

(1) The "004010" is a much more hierarchical structure than the "003051" which is more sequential in its composition, and

(2) The "004010" is predicated on a true standard implementation guide that provides considerably more detail and rigidity to the claim transaction. This detail and rigidity is where the greatest challenges lie, and it is what distinguishes provider operations today, from those that will be required after October 16, 2002.

Further confirmation that few, if any, providers are conducting standard transactions is offered through HIPAA's required use of standard code sets. Currently, most provider systems contain logic to create payer-specific coding to accommodate payer- or plan-specific code sets. These payer-specific codes will no longer be allowed and the system logic that produces those codes must be "unwound," payer by payer, to submit and receive HIPAA compliant transactions. The effect that this code set conversion will have is unclear. Providers should be assessing the impact that this code set conversion will have on reimbursement levels in an effort to arm themselves as they enter into negotiations to develop code set conversion strategies, or worse yet are simply told what the appropriate conversions will be. An example may help to clarify. If we assume a provider and a payer have contractually agreed to a fixed amount of payment for a particular service, however, this particular service has no ideal standard code so the provider submits a claim using a local code that has been agreed to by the provider and the payer. Let's assume the level of reimbursement for this particular service has historically been $50 per service. However, under HIPAA this unique coding arrangement is no longer acceptable, meaning the provider will have to identify the most appropriate code from the HIPAA approved standard code sets (CPT, HCPCS, ICD-9, etc.). The code that is identified may have a higher or a lower reimbursement than the previously used non-standard code. Few providers have gotten to this level of detail and many seem content to leave these issues to the payer to resolve. Providers should pursue these issues swiftly and aggressively, there are often many more codes than expected and their satisfactory resolution will take considerable time and require extensive coordination. Providers must be actively involved in the mapping of non-standard codes to national code sets, as this activity could have significant impacts on revenue and cash flow. Some providers have discussed allowing the clearinghouse or vendor to populate certain of these fields or to provide standard code set mapping tables. This practice, while feasible in some situations, creates the potential for considerable liability when diagnosis, procedure codes or other information is mapped inaccurately.

Finally, many providers have overlooked the need for testing. For example, testing is necessary for each category or type of health care transaction that a provider submits. Providers must conduct testing with each payer for a variety of transactions, not only for the data elements that are generally required, but also for the data elements that are required in special situations (The extent to which standard transactions and clearinghouses will obviate this need is still unclear). For example, durable medical equipment, ambulance claims, and anesthesia claims all require additional data elements that are not required in a claim for an office visit, and even a claim for a non-referred office visit is different from a claim for services based on a provider referral.

Although there is no specific requirement for testing of or compliance with the implementation guides and the related data, the Strategic National Implementation Process (SNIP) the workgroup constituted under the Workgroup for Electronic Data Interchange (WEDI) has recommended transaction testing prior to "going live" with standard transactions. This SNIP workgroup has recommended six mandatory and one optional level of testing[4].

[4] This issue of HIPAA compliance testing can be complicated, but in an attempt to clarify the testing issue we have included a summary of the various levels of testing, explained in laypersons terms, at Appendix II.

[5] In fact, ANSI ASC X12's proposal for the next generation of its transactions and code sets (version "004050") are currently underway and are expected to be delivered to HHS for consideration next year.

MYTH #4: "The industry will have had more than the required 24 months to implement administrative simplification."

REALITY:

Summary

This argument is misleading and mischaracterizes the HIPAA standards. There have been many significant proposed and approved changes to the HIPAA transaction standards and code set regulations. In fact, we are currently anticipating updates to certain standards as this document goes to print. What is more important to note is that final rules, in this instance, will not mean that there will be no additional changes to this component of HIPAA. While we understand why many have hesitated to start, we suggest that this normally prudent "wait and see" behavior is no longer acceptable in addressing HIPAA TCS regulations given the time remaining.

Supporting Information

This statement, although grounded in some historical facts, is both unrealistic—how many businesses, let alone businesses as cash-strapped as health care providers, implement expensive proposed regulations—and immaterial to the current state of health care industry readiness. The final transaction rule published August 17, 2000 had few changes from the proposed transaction rule published May 7, 1998. With 17,000 comment letters on the draft rules, however, who could have been certain as to the exact content of the final rule? In hindsight, it may be true that if most covered entities had taken the risk and begun to implement the proposed rule, they would only have had to make minor changes to adjust for the final transactions rule and implementation guides. However, health industry participants had more than enough final regulatory issues (e.g., OIG, APCs, GLBA and state laws) to make implementing proposed and uncertain rules unlikely and arguably unwise.

The above statement also mischaracterizes the standards. None of the transactions have been tested yet in the multiplicity of environments of the health care industry, and all are in a perpetual process of change. Like all HIPAA rules, the transaction rule can undergo annual changes to accommodate industry needs. For example, adjustments to the implementation guides will be issued shortly after publication of this article to the most familiar of HIPAA standards, the formats for claim submission (837I and 837P). The rules are designed to be a living document, capable of evolving and incorporating changes to accommodate the health industry[5].

The need for change and obstacles to change is more apparent in connection with areas of more specialized services. The home health care environment uses specialized codes that are not currently available in the HIPAA mandated code sets (i.e., ICD-9-CM, CPT-4, HCPCS, etc.). The focus of many mental health programs on functional status may be frustrated because the required ICD-9 codes (unlike the current DSM4 codes) contain no such information. The recent controversy relating to the use of J-codes for prescription drugs does provide an argument for "watchful waiting" instead of commencing massive code remediation in controversial areas.

Hospitals expressed their concerns about the replacement of J-codes with the NDC codes, and that advocacy eventually led DHHS to permit J-codes under HIPAA.

Interestingly, the lack of finality of HIPAA standards has been used as an argument against extension in requiring compliance with the standard transactions and code sets.[6] Unfortunately, the current state of the healthcare industry casts significant doubt that the provider community will be assessed, implemented, tested and ready by October 16, 2002.

[6] See, e.g., Moran and Snyder, op. cit., p. 13.

MYTH #5: "Medicare already does it, therefore it should translate easily into other government and private pay situations."

REALITY:

Summary

While Medicare does use an earlier version of the claim transaction (837) and remittance transaction (835), it does not use all of the mandated HIPAA standards. Further, there are significant differences in the earlier versions of the claim (837) and remittance (835) transactions from the mandated HIPAA standard formats. As a result, Medicare also must make significant investments to achieve HIPAA compliance. Compared to private payers, Medicare's changes, while extensive, are less complex than those faced by private payers and Medicaid. However, providers will face substantial changes to their operations, including collecting and submitting many new and different data elements (including those not currently needed for Medicare) and using all the standard medical and non-medical codes in order to submit HIPAA compliant claims and other transactions to Medicare.

The Medicare program's use of ANSI X12N standards for some transactions does not constitute a basis of comfort for providers engaged in certain electronic transactions with Medicare and seeking to move to HIPAA compliant transactions. To be compliant, HIPAA standard transactions (except for retail pharmacy, which utilizes an entirely different standard known as NCPDP) must not only conform to the ANSI X12N version 4, release 1, sub-release 0 ("004010," as opposed to the much more widely used version "003051," the version currently utilized by Medicare), but must also conform to the appropriate HIPAA transaction implementation guide. Many differences between Medicare's implementation of the ANSI transactions and the requirements of HIPAA's implementation guides exist, and the differences even among the Medicare's implementation of the ANSI standards are significant. The largest difference between Medicare and non-Medicare transactions for HIPAA implementation purposes is the degree of centralization and uniformity of Medicare systems. Non-Medicare systems, by contrast, often have to deal with many conflicting legacy systems, as well as local and client-specific requirements not faced by the Medicare program, including many "workarounds" designed to address the needs of a particular customer, particular provider or particular market.

Supporting Information

The Medicare program's use of X12 standards for some transactions is offered by some as a basis for comfort both to providers engaged in some electronic transactions with Medicare and to carriers attempting to implement X12N. These arguments have a number of flaws:

First, as noted earlier, there is often a great deal of difference between performing ANSI X12N transactions and performing those transactions according to the newly authored HIPAA implementation guides. The current Medicare carrier implementation guides are not based on the HIPAA standard implementation guides. This means that the X12N 837 implemented by Medicare are based on the data content of the NSF and UB92 formats. Thus, Medicare may actually be closer to the more traditional NSF and UB92 implementation guides than it is to the HIPAA implementation guides.

Secondly, even though Medicare carriers conduct the X12N 837 claim transaction, there are significant variances between the Medicare's various implementation guides. Thus an 837 transaction sent to one Medicare carrier would differ from an 837 transaction sent to another Medicare carrier. These differences exist notwithstanding the relative uniformity of Medicare systems compared to those of private carriers.

Perhaps the largest difference between Medicare and commercial carriers for HIPAA implementation purposes is the degree of centralization and uniformity of Medicare systems. For example, Medicare facility claims are processed on one of two primary systems: The Arkansas system ("APASS") and the Fiscal Intermediary Shared System ("FISS" – formerly referred to as the Florida Shared System 'FSS'). This centralized processing for such a large block of business makes Medicare's transition to HIPAA transactions simpler than that of even a tiny carrier with a complex aggregation of legacy systems, because in HIPAA transactions the labor varies more directly with the type and number of systems than with the volume of activity. Whether a provider sends a thousand claims a year or millions of claims per year does not significantly alter the assessment and remediation work associated with the systems to which the claims are sent.

Medicare receives most claims electronically today. On the Medicare Part A side (hospital and institutional bills), 98 percent of claims are submitted electronically; while more that 80 percent of Medicare Part B claims (physicians, professional and non-institutional bills) are submitted electronically. If even a small percentage of providers revert to paper because of the complexity of converting to HIPAA standard transactions, the Medicare system could face a potential crisis. If Medicare were flooded with significantly increased volumes of paper, providers are likely to face long delays in payment, as the Medicare system is not staffed or funded to handle a sudden large influx of paper claims,

By contrast to Medicare, most commercial insurers must deal with many legacy systems and unwind many "workarounds" designed to address the needs of a particular customer, particular provider or particular market. Inconsistent local, client-specific or provider-specific requirements are much less common for the Medicare program, which has historically achieved more standardization due to its more centralized operating environment and market power.

MYTH #6: "HIPAA compliance will be much simpler for small providers."

REALITY:

Summary

The evidence does not support this statement. In fact, some have suggested that their issues may be more challenging. Small providers are often, even today, unaware of HIPAA and the magnitude of its effects.

The only basis for this argument that compliance will be much simpler for small providers seems most often linked to the ability of small providers to revert to paper/manual transactions. This course of action may prove comforting in the short-term, but over the long-term may prove to be crippling. In fact, CMS has indicated that they may begin charging a fee for the processing of paper claims submissions, which would likely open the door to fees being charged by all healthcare payers.

Supporting Information

The challenges of HIPAA compliance for small providers are often glossed over by saying that since their systems and problems are less complex than those of large providers, they will deal with HIPAA through simple solutions provided by vendors.[7] While less complex, these small providers will need to go through the same exercises that large providers will need to go through to ensure that they are able to generate HIPAA compliant transactions. In fact, some would argue that small providers are hit harder than large providers, in that they do not have the economies of scale to implement these substantial regulatory requirements. While HIPAA's privacy and security regulations address the concept of scalability, softening the impact for smaller organizations, the idea of scalability in TCS is not feasible – an organization will either be able to submit and/or receive a compliant transaction or it will not. As a practical matter, although certainly not recommended or preferred, this situation may force some providers to revert to the expense and delay of paper transactions.

Unlike the institutional providers, which tend to use one or more of the major systems, many physician practices have used practice management software developed by smaller companies or by weakened or departed practice management companies. Like Y2K, HIPAA may drive significant consolidation among physician practice management software vendors. One should be concerned that the lack of operational readiness of physician practices, together with the transition costs associated with such consolidation, may lead some smaller providers to revert to paper submission of claims as their only safe alternative for the moment. We hope vendors serving this market exceed our expectations and provide true HIPAA solutions soon. We do believe, however, that the standardization for which HIPAA provides will ultimately lead to better and more cost-effective solutions for this marketplace. Our concern is whether the supply will be ready to meet the timing of the demand and whether these providers will be receptive to, and capable of making the necessary changes by October 16, 2002.

[7] See, e.g., Moran and Snyder, op cit., p. 16.

Despite the recognition by DHHS of the significance of the task of physician HIPAA compliance, very little effective action has been taken. Education campaigns for small providers are often locally driven, and do not exist in many areas. With no appreciable government support, small providers will look to commercial entities for support. Entities that really want to help the physicians get ready for HIPAA—and have strong incentives to do so—are often the large integrated delivery networks, but they rightly avoid offering anything of value to physicians due to Stark and anti-kickback concerns.

MYTH #7: "State governments only need to worry about Medicaid and their state employee group health plans."

REALITY:

Summary

State governments are coming to realize the broader impact of HIPAA. In fact, the National Governors Association (NGA) recently noted that "all state agencies that collect health data, provide or pay for health services, conduct research, or develop health policy will need to comply with HIPAA uniform standards in order to conduct business and protect public health." Few states or federal agencies have assessed the impact of HIPAA in this manner, or budgeted for an assessment or for the changes that will soon be required. Many government agencies, instead of carefully analyzing the information they can get through the new standard transactions, will simply impose new reporting requirements outside of the HIPAA standard transactions. As a result, in addition to the efforts required for HIPAA compliance, providers will need to be educated and will need to develop new procedures to comply with these new government reporting processes and requirements.

Supporting Information

The major misunderstanding that state governments have needed to overcome is the notion that only their Medicaid programs and state employee group benefit plans are affected by HIPAA. State governments have been confronting the requirements of Administrative Simplification for some time, but only recently have many states faced the many ripples associated with HIPAA that go well beyond the agencies explicitly covered by HIPAA. This awareness led the National Governor's Association to take a position in favor of HIPAA extension,[8] and led the Governor of Indiana to write a strongly worded letter attacking HIPAA as an unfunded mandate that will impact approximately 60 state agencies at a cost of approximately $100 million (excluding Medicaid)[9] As this article is being written, press reports indicate that the National Governor's Association has expanded its arguments for extension to include the argument that the communication with providers needed for the close monitoring of bioterrorism threats is jeopardized by HIPAA implementation.

The full impact of TCS is only beginning to be understood by federal, state and local government agencies that develop or implement policy—not only in the health care arena but, e.g., environmental, transportation, community development and workforce policy—analyze health data, conduct or fund research, regulate the health system or provide or pay for services. Such agencies will need to make systems and business process changes consistent with HIPAA standards in order to continue to communicate with health industry participants, to gather information from them, to monitor their performance and to regulate them.

[8] Letter from the National Governor's Association of August 22 to Chairman Baucus, Senator Grassley, Chairman Tauzin, and Repre sentative Dingell.

[9] Letter to Senator Bayh of July 16. Governor O'Bannon specifically claims that HIPAA Without understanding all of the types of information available through HIPAA standard transactions, skirted the Unfunded Mandates Reform Act by not stating its mandates "explicitly," and notes that "states that do not implement the proposed system changes will find it virtually impossible to communicate with insurance companies and providers.

Many such agencies will choose to impose new reporting structures outside of HIPAA onto health industry participants, increasing administrative costs in the system. Not only, as the NGA suggests, do stringent transaction requirements for health industry participants pose a significant challenge to the rapidly expanding role of public health surveillance, but a standard transaction system with new elements focused on public health monitoring needs would greatly enhance the effectiveness of such surveillance. The budgets of few government agencies reflect their needs and opportunities in connection with TCS. Although we have heard no concerns expressed by federal agencies that parallel the concerns of the NGA, neither have we seen strong evidence that federal agencies, including both health and non-health agencies, have budgeted and begun readying themselves for HIPAA.

Although this article does not otherwise address HIPAA's privacy and security regulations, we offer Appendix III as a means of helping the reader to identify the breadth of HIPAA's impact on state government. All states will differ, of course, with respect to specific agencies and functions affected by HIPAA.

MYTH #8: "HIPAA compliance equals administrative simplification."

REALITY:

Summary

This statement is simply not true; compliance can be obtained without realizing any operational efficiency or simplification. For that matter, compliance could be obtained while becoming less efficient and more complex. HIPAA offers no guarantees for improved efficiency or administrative simplification; these things will only come to those who seek them carefully and diligently. Make no mistake: HIPAA is a watershed event for the healthcare industry, but there are no assurances that its benefits will be evenly distributed; instead, they will cluster around those organizations that are most effectively prepared for them.

Supporting Information

The most successful and valuable HIPAA implementations we have seen to date are beingperformed by organizations that integrate simultaneously the requirements and opportunities of HIPAA into their strategic planning. Providers should approach the standard transactions with their eyes open to the potential for improved operations. With this goal in mind, we want to end this article with a very positive view of the potential of the standard transactions and code sets for provider business practices. This scenario may not be something that most provider organizations may adopt in whole cloth at this stage in their evolution toward electronic medical records (today only a small percentage of providers have implemented electronic medical records), but it will not happen if we do not at least envision it. Take, for example, the following future operating environment, which incorporates the benefits of most of the transactions:

a. The night before services are to be performed, a hospital is able to run a batch eligibility check on all out patients to be seen the following day. Based on this eligibility check, the hospital is made aware of specific change in several patients' insurance status. The failure to recognize these changes would have led to delays in payment that will now be avoided, not to mention the time saved by the many support staff who avoided time consuming phone calls to verify eligibility with each unique payer and government entity.

b. Automated authorization requests are sent out for all patients for whom such requests are required. Although fewer payers are requiring authorizations, this will still provide savings, to have the authorization in house ahead of time and in an electronic format.

c. Since the authorization is received electronically, it contains certain information that starts to populate the standard claim form. This functionality has led to reduced labor on an already over-worked staff and has improved the accuracy of data entry as keying errors are considerably reduced.

d. Services are rendered and an electronic claim is submitted. The same day the provider receives an acknowledgement that the claim has been received by the provider and has passed at least some preliminary format and content edits.

e. A pre-determined number of days after submission of the initial claim, a status inquiry is automatically sent to the payer to determine the status of the claim.

f. The on-line response indicates the claim has suspended for additional chart notes, these notes are collected and forwarded immediately to the payer. In the future, these clinical information requests may trigger automated responses, as electronic medical records become more common and more standardized. In the near future, these additional chart notes may be forwarded electronically via HIPAA's much anticipated health claim attachment transaction (275).

g. The payer, having gotten the appropriate information from the provider in a more timely fashion, is in turn able to adjudicate the claim.

h. Payment is sent electronically to the provider's bank account, while at the same time the remittance advice is delivered directly to the provider electronically. This enables the provider to get money deposited into the appropriate account more quickly, and has saved considerable labor expense as the provider did not need to incur the historic expense of posting the paper EOB.

i. Utilizing the newly standardized data, the provider is also able to establish and automated mechanism to review each remittance and assess that payment has been made in accordance with the applicable contract. An exception report is generated, to address any payment discrepancies. The collection department statistics improve as they become more focused and have more reliable data.

For HIPAA to yield its benefits, we need to shift the focus of HIPAA implementation from compliance with complex requirements to the opportunities for operational improvements and long-term business strategies.

We need to build in planning for the power and capacity needed for the inevitable transition from an X12 environment to an XML environment, and for the many uses of electronic records databases in research, quality improvement and medical safety. The anticipated health claims attachment standard will pave the way for the connection of purely administrative transactions to the clinical systems and the growing use of digital clinical information. The health claims attachment transaction (275) (standards not yet issued by HHS) adopts standard clinical nomenclature, and these standards may prove to be the linkage that allows standardization to

bridge across administrative and clinical systems. This bridging of administrative and clinical systems will provide the healthcare industry with even greater tools to generate substantial cost savings, improve the quality of care and enhance medical safety in our healthcare system. Organizations that view HIPAA in this way are making HIPAA implementation a much more valuable and strategic process than a simple compliance exercise.

With the looming compliance date, however, we are concerned that many organizations will be forced to simply opt for basic compliance, and at this late date many may struggle even to attain basic compliance. In any event, for most organizations, HIPAA will be something of a self-fulfilling prophecy. If they see it as added government regulation with no upside, that is what it will be. Alternatively, if they see it as an opportunity to improve their competitive position, it will be just that. Once this basic determination is made, the scale of their success or failure will be predicated largely on their time and commitment to implementation. Organizations have little to lose—and much to gain—from approaching HIPAA as a foundation for strategy.

Appendix I - HIPAA CLAIMS TRANSACTION – INSTITUTIONAL

"Always Required" Fields

The following represents the detail listing of 126 fields that are always required in a compliant 837I (Institutional claim transaction). However, never will these 126 fields provide enough information on their own to generate a compliant claim transaction. There are over 900 fields that may potentially be required to generate a compliant transaction. The actual number varies of fields required will vary depending on the unique situation and supporting information of the claim(s) being submitted.

HIPAA Field Name

Assigned Number
Benefits Assignment Certification Indicator
Benefits Assignment Certification Indicator
Billing Provider Address Line
Billing Provider City Name
Billing Provider Identifier
Billing Provider Last or Organizational Name
Billing Provider Postal Zone or ZIP Code
Billing Provider State or Province Code
Claim Frequency Code
Claim or Encounter Identifier
Communication Number
Communication Number Qualifier
Contact Function Code
Date Time Period Format Qualifier
Date Time Period Format Qualifier
Date Time Qualifier
Entity Identifier Code
Entity Identifier Code
Entity Identifier Code
Entity Identifier Code
Entity Identifier Code
Entity Identifier Code
Entity Identifier Code
Entity Identifier Code
Entity Identifier Code
Entity Type Qualifier
Entity Type Qualifier
Entity Type Qualifier
Entity Type Qualifier
Entity Type Qualifier
Entity Type Qualifier
Entity Type Qualifier
Entity Type Qualifier
Explanation of Benefits Indicator
Facility Code Qualifier
Facility Type Code
Hierarchical Child Code
Hierarchical Child Code
Hierarchical ID Number
Hierarchical ID Number
Hierarchical Level Code
Hierarchical Level Code
Hierarchical Parent ID Number
Hierarchical Structure Code
Identification Code Qualifier
Identification Code Qualifier
Identification Code Qualifier
Identification Code Qualifier
Identification Code Qualifier
Individual Relationship Code
Information Receiver Identification Number
Laboratory or Facility Address Line
Laboratory or Facility City Name
Laboratory or Facility Postal Zone or ZIP Code
Laboratory or Facility State or Province Code
Line Item Charge Amount
Medicare Assignment Code
Originator Application Transaction Identifier
Other Insured Identifier
Other Insured Last Name
Other Payer Attending Provider Identifier
Other Payer Last or Organization Name
Other Payer Operating Provider Identifier
Other Payer Other Provider Identifier
Other Payer Primary Identifier
Other Payer Referring Provider Identifier
Other Payer Service Facility Provider Identifier
Patient Account Number
Patient Address Line
Patient Birth Date
Patient City Name
Patient First Name
Patient Gender Code
Patient Last Name

Patient Postal Zone or ZIP Code
Patient State Code
Payer Identifier
Payer Name
Payer Responsibility Sequence Number Code
Pay-to Provider Address Line
Pay-to Provider City Name
Pay-to Provider Postal Zone or ZIP Code
Pay-to Provider State Code
Procedure Code
Product or Service ID Qualifier
Provider Code
Provider Code
Provider Code
Provider Taxonomy Code
Provider Taxonomy Code
APPENDIX I
Provider Taxonomy Code
Receiver Name
Receiver Primary Identifier
Reference Identification Qualifier
Reference Identification Qualifier
Reference Identification Qualifier
Reference Identification Qualifier
Reference Identification Qualifier
Reference Identification Qualifier
Reference Identification Qualifier
Reference Identification Qualifier
Related Causes Code
Release of Information Code
Release of Information Code
Responsible Party Address Line
Responsible Party City Name
Responsible Party Postal Zone or ZIP Code
Responsible Party State Code
Service Line Revenue Code
Service Unit Count
Statement From or To Date
Submitter Contact Name
Submitter Identifier
Submitter Last or Organization Name
Subscriber Last Name
Total Claim Charge Amount
Transaction Segment Count
Transaction Set Control Number
Transaction Set Control Number
Transaction Set Creation Date
Transaction Set Creation Time
Transaction Set Identifier Code
Transaction Set Purpose Code
Transmission Type Code
Unit or Basis for Measurement Code

Appendix II - HIPAA STANDARD TRANSACTION AND CODE SETS

Testing Levels - Explained

Level 1-Integrity Testing

Testing for HIPAA Implementation-guide-specific requirements as repeat counts, used or not used codes, elements and segments, required or intra-segment situational data elements, non-medical code sets as identified in the implementation guides. **– This means that the transaction set adheres to the HIPAA implementation guides. The implementation guides specify which segments and data elements are required or not used (a "not used" segment would be allowed by the X12 standard, but would not be valid based upon the implementation guide). They also specify the order in which the segments and data elements must be presented in order to be a compliant transaction. Implementation guide requirements also limit the valid values of many data elements (e.g., a date/time qualifier would have hundreds of values in the standard, but the implementation guide restricts valid values - such as, first date of service, last date of service, discharge date, etc.). This is referred to by some as a "restricted view" of the standard (view of the standard based in the implementation guide).**

Level 2-Requirement Testing

Testing for HIPAA Implementation-guide-specific requirements as repeat counts, used or not used codes, elements and segments, required or intra-segment situational data elements, non-medical code sets as identified in the implementation guides. **- This means that the transaction set adheres to the HIPAA implementation guides. The implementation guides specify which segments and data elements are required or not used (a "not used" segment would be allowed by the X12 standard, but would not be valid based upon the implementation guide). They also specify the order in which the segments and data elements must be presented in order to be a compliant transaction. Implementation guide requirements also limit the valid values of many data elements (e.g., a date/time qualifier would have hundreds of values in the standard, but the implementation guide restricts valid values - such as, first date of service, last date of service, discharge date, etc.). This is referred to by some as a "restricted view" of the standard (view of the standard based in the implementation guide).**

Level 3-Balancing

Testing of the transaction for balanced field totals, record or segment coupling, financial balancing of claims or remittance advice, and balancing of summary fields. **- Transaction sets, particularly the remittance advice (835) and premium payment (820) have internal financial balancing segments to support electronic funds transfer. The HIPAA implementation guides require the detail lines to balance to the claim lines and then to the total claim amount. The sum of the claim amounts must also balance up to the total remittance amount. The balancing also accounts for adjustments to the claim and payment.**

Level 4-Situation Testing

Testing of specific inter-segment situations described in the HIPAA Implementation guides such that if element A occurs than element B must be populated. This is considered to include the validation of situational fields given values or situations presented and identified within the transaction. **- The situational segments and data elements are used according to the implementation guides. A simple example is that the country code should be provided only in cases where the address is outside of the U.S. Other situations would be that one data element is required if another data element is provided. In all cases, the authors of the implementation guides have tried to clearly identify the situations for use.**

Level 5-Code Set Testing

Testing for valid implementation guide specific code set values. **- Only valid values of external data elements are used. For example, only valid codes contained in the named code set such as ICD-9, CPT-4/HCPCS, etc. are used. The valid values are not specified within the implementation guides, but are published by external sources. Another example is that on the National Provider ID is developed, only valid National Provider IDs are used to identify providers, as opposed to HIC Numbers, TINs, SSNs, Medicaid numbers, etc.**

Level 6-Specialty or Line of Service Testing

Specialized testing required for certain healthcare specialties. **- The data is valid based upon healthcare standards and specialty situations. Examples would include no C-section procedures on males, no pediatric specific diagnoses for patients over 18, not heart transplants in an outpatient setting, etc. Another example would be if an institutional claim had a bill type indicating it was a home health claim. You could expect the home health segments of the claim to be present (based on the situational usage of those segments).**

Optional Level 7-Trading Partner Testing and Evaluation

Testing of trading partner's ability to transmit HIPAA Compliant data. **- This is testing of the telecommunication interface and also of specific trading partner requirements. In Level seven we see testing that determines whether or not the trading partner is able to deliver the transaction set to the correct electronic mailbox(es). This includes testing of communication protocols, security requirements (encryption, passwords, etc.) and should include testing response to the transaction - the functional acknowledgement (X12 997).**

At this level we also see trading partner specific edit testing. Trading Partner specific editing occurs when one of the trading partners has identified specific edits (within the scope of the HIPAA IG requirements) and they are validating based on this level of specificity. For example, if a payer only has member numbers that start with "123" they could set an edit to say if member number in the NM1 doesn't start with "123" it's not our member – and either reject the claim or send it to a work queue. Another example of this is when a payer may restrict the number of claims per transaction set due to systems limitations (the recommended limit is 5,000 claims per transaction set). A payer's translator may only be able to process 2,500 claims at a time (some translators are memory based and are restricted in the file sizes that they can process). This is not considered a modification to the implementation guide.

Appendix III - HIPAA's IMPACT ON STATE GOVERNMENTS

Provider Functions	Health Plan and Clearinghouse Functions	Other Areas Requiring Review, Education, and Some Change
❖ State University Medical Centers ❖ State, County and Municipal: ➢Hospitals ➢Clinics ➢Mental health services ➢Substance abuse services ➢Emergency medical services ➢Disaster preparedness programs ➢Correctional facility health services ➢Developmental disability services ➢Direct services to the blind and other disabled populations ➢Direct services to the elderly and children ➢Health screening and other preventive programs ➢Refugee services ➢Rural health services ➢Community healthcare partnerships with substantial governmental involvement ➢Welfare and other social service programs involving health services or health information ➢Other programs employing health practitioners licensed as such by the State or defined as providers under the Social Security Act	❖ Medicaid ❖ State Employee and Retiree: ➢Group medical plans ➢Long term care plans ➢Prescription drug plans ➢Dental and vision plans (unless very limited) ➢Flexible spending accounts ➢COBRA coverage ➢Disease management and intervention programs ❖ Human Resources Functions in All Agencies: ➢Fitness for duty exams ➢Pre-employment physicals ➢Health promotion and disease prevention programs ➢Employee assistance programs ➢Absenteeism studies ➢Health and productivity programs ➢Workplace medical and safety surveillance ❖ Children's Health Insurance Programs ❖ Medicaid Expansion Programs ❖ Many Welfare And Other ❖ Social Services Benefits Programs ❖ Mental Health Benefits Programs ❖ Some State-Sponsored ❖ Student Health Insurance Programs ❖ Third-Party Administrator functions ❖ Clearinghouse functions ➢For federal programs involving health information ➢Coordination of benefits	❖Registries for Diseases (e.g., cancer, AIDS) and Disease Prevention (e.g., immunizations) ❖State And County Public Health Agencies ❖Regulators of Health Professional and Facility Licensure ❖State, County and Municipal Law Enforcement ❖Departments of Corrections ❖Civil Rights Regulators ❖Protective Services Agencies (Foster/Adoption/Abuse) ❖State Insurance Department and Other Regulators of MCOs and of External Review ❖State Departments Of Elder Affairs and Area Agencies On Aging ❖Workers' Compensation Commission and Labor Dept. ❖Other Social Service Agencies ❖State Technology Regulators ❖State Health Information Databases ❖Organ Procurement Programs ❖Minority Health Programs ❖Rural Health Programs ❖Federally Qualified Health Centers ❖Business Associates (much too numerous to list, but including): ➢Systems vendors ➢Attorneys ➢Consultants ➢Auditors ➢Peer Review Organizations ➢Third Party Administrators ➢Clearinghouses ➢Pharmacy Benefit Managers ➢Utilization Management Firms

www.pwcglobal.com/healthcare

Your worlds  Our people